

CASE NO.: AM9-99-0138
Serial No.: 09/487,502
March 6, 2004
Page 9

PATENT
Filed: January 19, 2000

Remarks

Reconsideration of the above-captioned application is respectfully requested. All pending claims (1-35) have been rejected as being unpatentable over Atjai/Dwork in view of Diffie-Hellman, and indefiniteness rejections have been lodged against the independent claims for allegedly reciting relative terms. As now amended, the claims have broadened to remove the allegedly relative terms, so only the obviousness rejections remain at issue.

Amended independent Claim 1 recites in part that the message μ (or a concatenation thereof) is mapped to a message point "x" in n-dimensional space using a function "f" which renders infeasible the possibility of mapping two messages together in the N-dimensional space. Amended independent Claim 19 also recites in part mapping the message μ to a message point "x" at which it is not feasible to map any other message. Amended independent Claim 12, on the other hand, recites in part finding a point "y" of a key lattice \mathcal{L} that is not the same as the auxiliary lattice on which the point x is located, as disclosed in Figure 2 (the message point x returned by the logic cannot be part of the key lattice). Amended independent Claim 26 further specifies that the message μ or a concatenation thereof is mapped to a message point "x" in n-dimensional space, with the message point "x" being an element of a set of spaced-apart points that are not on the lattice.

Claims 1-35 remain pending.

Rejections Under 35 U.S.C. §103

1053-73.AMD

CASE NO.: AM9-99-0138
Serial No.: 09/487,502
March 6, 2004
Page 10

PATENT
Filed: January 19, 2000

Claims 1-35 have been rejected under 35 U.S.C. §103 as being unpatentable over Atjai/Dwork in view of Diffie-Hellman. Consider first the difference between Atjai/Dwork and the present invention, which has been missed by the examiner. Atjai/Dwork teaches a cryptographic system that uses the hardness of lattice-solving problems to generate a public key/private key pair. That such existed prior to filing the present application is taught in the present background, as is the problem with such systems: potentially, two messages undesirably could be mapped close together, see page 2, first full paragraph ("unfortunately, the scheme disclosed by Goldreich et al., as admitted by Goldreich et al., might result in mapping two messages close together in the n -dimensional space, which would defeat the scheme as to those two messages because both messages would have the same digital signature").

In contrast, the present claims distinguish over previous lattice-based crypto key systems such as Atjai/Dwork by ensuring that the noted problem does not occur. Specifically, Claims 1 and 19 recite that the message point "x" is selected so that it is infeasible to map two messages together, something not taught or recognized in Atjai/Dwork, and Claims 12 and 26 recite specific modalities for achieving this (respectively, finding a point "y" of a key lattice \mathcal{L} that is not the same as the auxiliary lattice on which the point x is located, and specifying that the message μ or a concatenation thereof is mapped to a message point "x" in n -dimensional space, with the message point "x" being an element of a set of spaced-apart points that are not on the lattice.)

None of these differences between the present claims and Atjai/Dwork have been specifically addressed in the Office Action. More particularly, the rejections do not contend that Atjai/Dwork achieves or even suggests the stated result of Claims 1 and 19, much less by using the particular modalities of Claims 12 and 26. Diffie-Hellman (discussed further below), for instance, has been used only for its teaching of

1033-73.AMD

CASE NO.: AM9-99-0138

Serial No.: 09/487,502

March 6, 2004

Page 11

PATENT

Filed: January 19, 2000

digital signatures in the rejection of Claim 1. Accordingly, since it has not been shown where every claim element is in the prior art or the general level of skill in the art, the claims are patentable, MPEP §2143.01.

Turning to the combination of Diffie-Hellman with Atjai/Dwork, there is absolutely no prior art motivation to make the combination, much less any prior art suggestion of success in doing so, in contravention to MPEP §2142. The reason is easy to see why. Atjai/Dwork is directed to one way for obtaining a public key/private key pair (using hard problems of lattices) whereas Diffie-Hellman is directed to another way that is virtually orthogonal to lattice methods, namely, by factoring a large number obtained as a product of two large prime numbers. No evidence has been produced that, unlike unified field theories that have attempted to combine general relativity with quantum mechanics, anyone ever attempted, much less suggested, generating public key/private key pairs by combining lattice-based techniques with factoring two prime numbers. This explains the incoherence of the proffered rationale on page 5 of the Office Action to combine these two wildly disparate techniques, as well as laying bare the fallacies underpinning the rejections of various dependent claims (e.g., the allegation regarding Claim 5 that "Diffie-Hellman disclose for the functions suitable for f sparse polynomials over finite field. Thus f maps μ to a point in the range space of f " (sic)). Using this enigmatic allegation as but one example, it is doubtful whether very much of the explanation of the rejections would be comprehensible, much less persuasive, to the Board, who can be counted on to recognize the gulf between Diffie-Hellman's prime number factorization scheme and Atjai/Dwork's lattice method and, hence, the lack of any rational expectation of success in combining the two.

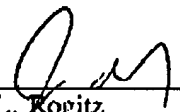
The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

1033-73.AMD

CASE NO.: AM9-99-0138
Serial No.: 09/487,502
March 6, 2004
Page 12

PATENT
Filed: January 19, 2000

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-72.AMD